



Wycliffe Church of England Primary School

E-Safety Policy

2019/20



Approved by the governing body: January 2020

Date for review: Feb 2021

Read annex c – KCSin E
Statement needed

RSE

Vision Statement

“Life in all its fullness” (John 10:10)

Our vision is to ensure that our school family are happy and fulfilled in a creative learning environment. This will be flexible and cater to individual needs and develop a love for learning through which all members can flourish. Our priority is to nurture habits and accountability which lead to sustainable development and responsibility.

E-Safety Co-ordinator – D Baxter

ICT Co-ordinator – K Bailey

Safeguarding Governor - G Denison

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. Wycliffe CE Primary School endeavours to highlight benefits and risks of using technology and provides safeguarding protocol and education for users to enable them to control their online experience.

Links to other policies and national guidance

The following school policies and procedures should also be referred to

- Safeguarding Policy
- Whistleblowing policy
- Behaviour Policy
- Guidance on Safer Working Practice
- Staff code of conduct
- Data Protection

The following local/national guidance should also be read in conjunction with this policy:

- Bradford Education and Safeguarding Team: Guidelines and Procedures (2019)
- PREVENT Strategy HM Government
- Keeping Children Safe in Education DfE September 2019
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils' lives, not just in our school but outside as well. As a school community we value all God's children and therefore we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

- We will provide a curriculum/Jigsaw curriculum/other lessons which has E-Safety related lessons embedded throughout.
- We will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant E-Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age-appropriate and supports the learning objective for specific curriculum areas.
- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind pupils about their responsibilities through an Acceptable Use Policy which every pupil will sign and be displayed throughout the school.
- School will model safe and responsible behaviour in their own use of technology during lessons.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying. See Anti-Bullying Policy.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline.

Staff Training

Our staff receive regular information and training on E-Safety issues, as well as updates as and when new issues arise.

- As part of the induction process all staff receive information and guidance on the E-Safety Policy, the school's Acceptable Use Policy, e-security and reporting procedures.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff will be encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access (Support Primary T)

- The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT system and that such activity will be monitored and checked.
- At Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises. They will ensure that they log out after each session.
- At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure. They will ensure that they log out after each session.
- All internet access will be undertaken alongside a member of staff or, if working independently, a member of staff will supervise at all times.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password. They will abide by the school AUP at all times.

Managing Filtering

- The school has the Smoothwall filtering system in place which is managed by the school and RM. Banned phrases and websites are identified.
- The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training/online safety lesson
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Co-ordinator immediately.
- If users discover a website with potentially illegal content, this should be reported immediately to the E-Safety Co-ordinator. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).
- Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the Headteacher/E-Safety Co-ordinator prior to being released or blocked.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

E-Mail

- Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

- Staff should not use personal email accounts for professional purposes, especially to exchange any school-related information or documents or to email parents/carers.
- Staff should not send emails to pupils.
- Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails.
- Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.
- Chain messages are not permitted or forwarded on to other school owned email addresses.

Social Networking

- Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'. Doing so will result in disciplinary action or dismissal.
- Schoolblogs or social media sites should be password protected and run from the school website with approval from the Senior Leadership Team.

Pupils Publishing Content Online

- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.
- Written permission is obtained from the parents/carers before photographs and videos are published.
- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use their own portable devices to store images/video/sound clips of pupils.

Mobile Phones and Devices

General use of personal devices

- Mobile phones and personally-owned devices will not be used in any way during lessons or school time. They should be switched off or silent at all times.
- No images or videos will be taken on mobile phones or personally owned devices.
- In the case of school productions, parents/carers are permitted to take pictures of their child in accordance with school protocols which strongly advise against the publication of such photographs on social networking sites.
- The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils' use of personal devices

- Pupils in Year 6 only who need to bring a mobile phone in to school can do so but this must be handed to the class teacher who will keep it secure until the end of the day. Children must not switch on their mobile phone until off school premises.
- Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- Mobile phones and personally -owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances. 3&4G must be turned off on the school premises.

General Data Protection (GDPR) and E-Safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to E-Safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information should only be sent by e mail when on a secure network.

Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the Trust's Data Protection Officer (DPO – P Thompson) immediately, who may need to inform the Information Commissioner's Office (ICO).

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any of school ICT resources.
- Come September 2020, all parents will be required to sign the home-school agreement prior to their children being granted internet access within school.
- All visitors and students will be asked to read and sign the Acceptable User Policy prior to being given internet access within the school.
- The school will maintain a current record of all staff and pupils who have been granted access to the school's internet provision.
- **Support for Parents**
- Parents' attention will be drawn to the school's E-Safety policy and safety advice in newsletters, the school website and E-Safety information workshops.
- The school website will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website will also provide links to appropriate online-Safety websites.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Co-ordinator). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment is a behaviour which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Our school follows and adheres to the national guidance - UKCCIS: *Sexting in schools and colleges: Responding to incidents and safeguarding young people*

Responses to Incident of Concern

An important element of E-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report E-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an E-Safety nature on cpoms.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities

Policy Review Date: February 2021 or when changes are necessary to comply with school policy or national legislation.

